Docket No.: 1509-493

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Katsuyuki YUMOTO

Serial No.: NEW

Filed: April 9, 2004

For: ACCESS CONTROL SYSTEM AND METHOD

CLAIM OF PRIORITY AND SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. §119, Applicant hereby claims the foreign priority benefit of Japanese Patent Application No. 2003-104756, filed April 9, 2003. A certified copy of the priority document is attached.

Respectfully submitted,

LOWE HAUPTMAN GILMAN & BERNER, LLP

Allan M. Lowe, Registration No. 19,641

1700 Diagonal Road, Suite 310
Alexandria, VA 22314
(703) 684-1111 Telephone
(703) 518-5499 Telecopier

Date: April 9, 2004

AML:rk

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月　９日

出願番号
Application Number: 特願２００３－１０４７５６

[ST. 10/C]: [ＪＰ２００３－１０４７５６]

出願人
Applicant(s): 日本ヒューレット・パッカード株式会社

２００４年　３月２２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０２３５０２

【書類名】　特許願
【整理番号】　200310074
【提出日】　平成15年 4月 9日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/00
【発明者】
　【住所又は居所】　東京都杉並区高井戸東３丁目２９番２１号　日本ヒューレット・パッカード株式会社内
　【氏名】　湯本　勝之
【特許出願人】
　【識別番号】　399117110
　【氏名又は名称】　日本ヒューレット・パッカード株式会社
【代理人】
　【識別番号】　110000039
　【氏名又は名称】　特許業務法人　アイ・ピー・エス
　【代表者】　早川　明
　【電話番号】　045-228-0131
【手数料の表示】
　【予納台帳番号】　132839
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　アクセス制御システムおよびその方法

【特許請求の範囲】

【請求項１】

オペレーティングシステムと、

前記オペレーティングシステムにより実行される１つ以上のプロセスそれぞれによる１つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置と

を含むアクセス制御システムであって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、

前記オペレーティングシステムは、

前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して、前記デバイスファイルそれぞれを生成するデバイスファイル生成手段と、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するアクセス規則設定手段と、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するアクセス制御手段と

を有し、

前記アクセス制御装置は、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を統一し、

前記アクセス制御手段は、前記アクセス規則が統一されたときには、前記統一されたアクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する

アクセス制御システム。

【請求項２】

１つ以上のプロセスそれぞれによる１つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置であって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

前記デバイスファイルそれぞれは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則が設定され、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスが制御され、

任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、

同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するアクセス規則抽出手段と、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するアクセス規則導出手段と

を有するアクセス制御装置。

【請求項３】

前記アクセス規則導出手段は、前記デバイスごとに抽出された複数のアクセス規則が異なっているときに、これら複数のアクセス規則のいずれかを、前記統一されたアクセス規則として導出する

請求項２に記載のアクセス制御装置。

【請求項４】

前記アクセス規則導出手段は、前記デバイスごとに抽出された複数のアクセス規則が異なっているときに、前記デバイスファイルとリンクされたファイルの属性に基づいて、前記統一されたアクセス規則を導出する

請求項２に記載のアクセス制御装置

【請求項５】

前記アクセス規則導出手段は、前記デバイスごとに抽出された複数のアクセス

規則が異なっているときに、これら複数のアクセス規則の内、前記デバイスファイルへのアクセスに対する制限が多いいずれかを、前記統一されたアクセス規則として導出する

請求項２に記載のアクセス制御装置

【請求項６】

前記プロセスはオペレーティングシステムにより実行され、

前記経路は、前記オペレーティングシステムが管理する１つ以上のディレクトリに存在し、前記プロセスそれぞれと前記デバイスファイルそれぞれとの間でリンクされた１個以上のファイルにより構成され、

前記アクセス規則は、前記デバイスファイルとリンクされたファイルが存在するディレクトリそれぞれに対して設定される

請求項２～５のいずれかに記載のアクセス制御装置。

【請求項７】

前記アクセス規則は、少なくとも、前記デバイスファイルにリンクされたファイルそれぞれが、前記デバイスファイルそれぞれに対する読み出しおよび書き込みそれぞれが許可されるか否かを示す

請求項２～６のいずれかに記載のアクセス制御装置。

【請求項８】

前記オペレーティングシステムは、前記アクセス規則を記憶し、

前記アクセス規則抽出手段は、前記オペレーティングシステムが起動されたときに、前記記憶されたアクセス規則から、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、

前記アクセス規則導出手段は、前記オペレーティングシステムが起動されたときに抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出する

請求項２～７のいずれかに記載のアクセス制御装置。

【請求項９】

前記オペレーティングシステムは、前記アクセス規則の変更を受け入れ、前記変更されたアクセス規則を、前記アクセス制御装置に通知し、

前記アクセス規則抽出手段は、前記アクセス規則の変更が通知されたときに、前記変更されたアクセス規則と関係する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、

前記アクセス規則導出手段は、前記アクセス規則の変更が通知されたときに抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出する

請求項２～８のいずれかに記載のアクセス制御装置。

【請求項１０】

１つ以上のプロセスそれぞれによる１つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御方法であって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

前記デバイスファイルそれぞれは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあり、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則が設定され、

同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出し、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する

アクセス制御方法。

【請求項１１】

１つ以上のプロセスそれぞれによる１つ以上のデバイスそれぞれに対するアクセスを制御するプログラムであって、

前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、

前記デバイスファイルそれぞれを、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成するステップであって、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあるステップと、

前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するステップと、

前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するステップと、

同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するステップと、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するステップと

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータのデバイスに対するアクセスを制御するアクセス制御システムおよびその方法に関する。

【０００２】

【従来の技術】

コンピュータのオペレーティングシステム（ＯＳ）として、ＵＮＩＸ（登録商標）が一般的に用いられている。

また、近年、このＵＮＩＸ（登録商標）をパーソナルコンピュータ向けにしたＬＩＮＵＸが普及している。

また、例えば、非特許文献１は、これらのようなＯＳの脆弱性を手当てする方法を開示する。

【０００３】

【非特許文献１】　"Compartmented mode operating system"（情報処理学会・第６５回（平成１５年（２００３年））全国大会講演論文集（５）・セクショ

ン２Ｔ９－４／５－５５５ページ）

【０００４】

【発明が解決しようとする課題】

本発明は、上述した背景からなされたものであり、コンピュータのＯＳの脆弱性を手当てして、その安全性を向上させることができるアクセス制御システムおよびその方法を提供することを目的とする。

【０００５】

【課題を解決するための手段】

［アクセス制御システム］

上記目的を達成するために、本発明に係るアクセス制御システムは、オペレーティングシステムと、前記オペレーティングシステムにより実行される１つ以上のプロセスそれぞれによる１つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置とを含むアクセス制御システムであって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、前記オペレーティングシステムは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して、前記デバイスファイルそれぞれを生成するデバイスファイル生成手段と、前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するアクセス規則設定手段と、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するアクセス制御手段とを有し、前記アクセス制御装置は、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を統一し、前記アクセス制御手段は、前記アクセス規則が統一されたときには、前記統一されたアクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する。

【０００６】

［アクセス制御装置］

また、本発明に係るアクセス制御装置は、１つ以上のプロセスそれぞれによる

１つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御装置であって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、前記デバイスファイルそれぞれは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則が設定され、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスが制御され、任意の前記デバイスそれぞれに対応して、複数のデバイスファイルが生成されることがあり、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するアクセス規則抽出手段と、

前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するアクセス規則導出手段とを有する。

【０００７】

［アクセス制御方法］

また、本発明に係るアクセス制御方法は、１つ以上のプロセスそれぞれによる１つ以上のデバイスそれぞれに対するアクセスを制御するアクセス制御方法であって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、前記デバイスファイルそれぞれは、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成され、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあり、前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則が設定され、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出し、前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出し、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御する。

【０００８】

［プログラム］

また、本発明に係るプログラムは、１つ以上のプロセスそれぞれによる１つ以

上のデバイスそれぞれに対するアクセスを制御するプログラムであって、前記プロセスそれぞれは、前記デバイスそれぞれに対応するデバイスファイルそれぞれを介して、前記デバイスそれぞれにアクセスし、前記デバイスファイルそれぞれを、前記プロセスそれぞれが、前記デバイスそれぞれにアクセスする経路それぞれに対応して生成するステップであって、前記デバイスファイルは、任意の前記デバイスそれぞれに対応して、複数、生成されることがあるステップと、前記経路それぞれに対して、前記デバイスファイルそれぞれにアクセスする方法を示すアクセス規則を設定するステップと、前記アクセス規則に基づいて、前記デバイスファイルそれぞれへのアクセスを制御するステップと、同じ前記デバイスに対応する前記複数のデバイスファイルそれぞれへの経路に設定されたアクセス規則を抽出するステップと、前記抽出されたアクセス規則から、前記デバイスごとに統一されたアクセス規則を導出するステップとをコンピュータに実行させる。

【０００９】

【発明の実施の形態】

[本発明の背景]

まず、実施形態の説明に先立って、その理解を助けるために、本発明にかかるアクセス制御方法がなされるに至った背景、および、本発明に係るアクセス制御方法の概要を説明する。

【００１０】

[デバイスへのアクセスの際に生じる問題]

図１は、本発明の背景を、具体例を挙げて説明する図である。

例えば、上述したＵＮＩＸ（登録商標）やＬＩＮＵＸなどと同様な処理を行うＯＳにおいては、実行中のプロセスが、コンピュータの記憶装置、インターフェースおよび出力装置などの資源（以下、「デバイス」とも記す）にアクセスするために、デバイスそれぞれに対応して設けられるデバイスファイル実体（以下、「デバイスファイル」とも記す）が用いられる。

【００１１】

つまり、例えば、図１に示すように、実行中のプロセスは、ディレクトリ”ａ／ｂ”の中の”ｆｉｌｅ＃１”を介して、”ｆｉｌｅ＃１”にリンクされたデバ

イスファイルにアクセスすることにより、デバイスへのアクセスを行う。

また、図１に同様に例示するように、実行中のプロセスは、ディレクトリ”ａ／ｃ”の中の”ｆｉｌｅ＃２”を介して、”ｆｉｌｅ＃２”にリンクされたデバイスファイルにアクセスすることにより、デバイスへのアクセスを行う。

【００１２】

ここで、あるデバイスファイルに対するアクセスについての規則（以下、アクセス規則とも記す）は、ディレクトリごとに決められる。

図１に示すように、例えば、ディレクトリ”ａ／ｂ”に対しては、デバイスファイルへのアクセスは、読み出し（ｒｅａｄ）のみが許可されるアクセス規則が設定される。

また、例えば、ディレクトリ”ａ／ｃ”に対しては、デバイスファイルへのアクセスは、読み出しおよび書き込み（ｒｅａｄ・ｗｒｉｔｅ）の両方がが許可されるアクセス規則が設定される。

なお、実際には、例えば、ディレクトリａに対しては、”ｒｏｏｔ”、ディレクトリｂに対しては”ｄｅｖ”、ディレクトリｃに対しては”ｔｅｍｐ”などの名称が付される。

【００１３】

このような場合、同じデバイスファイルにアクセスするのにもかかわらず、あるプロセスが、ディレクトリ”ａ／ｂ”にある”ｆｉｌｅ＃１”を介してデバイスファイルにアクセスするときには、デバイスファイルに対する読み出しのみが許可されるのに対して、ディレクトリ”ａ／ｃ”にある”ｆｉｌｅ＃２”を介してデバイスファイルにアクセスするときには、デバイスファイルに対する読み出しも書き込みも許可されてしまう。

このように、プロセスが、同じデバイスに対してアクセスする場合であっても、プロセスとデバイスファイルとの間でリンクされたファイルやディレクトリ（経路）をどのように選ぶかによって、適用されるアクセス規則が異なることがあると、プロセス処理上の矛盾が生じかねない。

【００１４】

[本発明の概要]

図２は、本発明の概要を、具体例を挙げて説明する図である。

なお、図２においては、デバイスが２つ、デバイスファイルが２つ、デバイスファイルにリンクされたファイルが２つ示されているが、これらの数は例示であり、また、ディレクトリも例示である。

従って、本発明に係るアクセス制御方法は、これらの数およびディレクトリ構成に限定されない。

また、図２に示されたアクセス規則は例示であって、本発明に係るアクセス制御方法は、この規則に限定されることはない。

【００１５】

このように、アクセス規則に生じる可能性がある不一致・矛盾を解決するためには、プロセス（１つとは限らない）が、同じデバイスにアクセスするときの経路それぞれにデバイスファイルを置き、これら複数のデバイスファイルに対するアクセス規則を統一すればよい。

具体的には、例えば、まず、図２に示すように、あるプロセスからデバイスにアクセスするための経路が複数あるときには、これらの経路それぞれにデバイスファイル（デバイスファイル＃１，＃２）を置く。

【００１６】

次に、これらのデバイスファイル＃１，＃２それぞれにアクセスするファイル（ｆｉｌｅ＃１，＃２）が存在する全てのディレクトリ（ディレクトリ”ａ／ｂ”，”ａ／ｃ”）から、デバイスファイル＃１，＃２にアクセスするためのアクセス規則が、ディレクトリ”ａ／ｂ”，”ａ／ｃ”の間で異なっているときには、これらのアクセス規則を統一し、例えば、書き込み（ｗｒｉｔｅ）を禁止し、読み出し（ｒｅａｄ）のみを許可する。

統一されたアクセス規則に従って、デバイスファイルに対するアクセスを行うことにより、ディレクトリ間のアクセス規則の不一致・矛盾が解消され、プロセス処理上の不具合が予防され、また、ＯＳの脆弱性を減ずることができる。

【００１７】

なお、ディレクトリ間のアクセス規則は、例えば、ＯＳのセキュリティを向上させるためには、図２に示したように、統一されたアクセス規則として、最も制

限が厳しいものを採用すればよい。

あるいは、例えば、ＯＳのパフォーマンスを向上させるためには、統一されたアクセス規則として、複数の経路の内、最も頻繁に用いられる経路のアクセス規則を採用すればよい。

あるいは、例えば、読み出し動作以外意味のないデバイスなど、デバイスに特徴がある場合、あるいは、経路に含まれるファイルに特徴があるときには、統一されたアクセス規則として、このファイルを含む経路によりデバイスにアクセスするために最適なアクセス規則を採用すればよい。

【００１８】

［第１実施形態］

以下、本発明の第１の実施形態を説明する。

【００１９】

［コンピュータ１］

図３は、本発明に係るアクセス制御方法が適応されるコンピュータ１のハードウェア構成を例示する図である。

図３に示すように、コンピュータ１は、ＣＰＵ１０２、メモリ１０４およびこれらの周辺回路などを含む本体１００、表示装置、キーボードおよびマウスなどを含む表示・入力装置１０６、ネットワークを介して他のコンピュータなど（いずれも図示せず）との通信を行う通信装置１１０、ＨＤ装置およびＣＤ装置などの記録装置１１２、および、記録装置１１２に対して着脱可能な記録媒体１１４から構成される。

つまり、コンピュータ１は、一般的なコンピュータとしての構成部分を有している。

なお、コンピュータ１の内、本体１００内に収容されたインターフェース、表示・入力装置１０６、通信装置１１０および記録装置１１２などが、図１，図２に示したアクセスの対象となるデバイスに相当する。

【００２０】

［ＯＳ２・第１のユーティリティプログラム３０］

図４は、図３に示したコンピュータ１上で動作するＯＳ２の構成と、本発明に

係るアクセス制御方法を実現する第１のユーティリティプログラム３０の構成を示す図である。

図４に示すように、ＯＳ２は、デバイスドライバ２０２－１～２０２－ｎ（ｎ≧１）、ファイルシステム２０４、デバイスデータベース（デバイスＤＢ）２０６、デバイスファイルＤＢ２０８、ディレクトリ管理部２１０、アクセス制御部２１２、規則ＤＢ２１４およびプロセス実行部２１６などから構成される。

また、第１のユーティリティプログラム３０は、デバイス番号生成部３００、検索部３０２、規則抽出部３０４および規則導出部３０６などから構成される。

【００２１】

なお、図４中に点線で示すように、ＯＳ２の規則ＤＢ２１４は、ユーティリティプログラム３０側に設けられていてもよい。

また、ＯＳ２の構成部分の分け方は例示であって、例えば、ファイルシステム２０４内に、デバイスＤＢ２０６などのデータベースが作成されてもよい。

また、以下、「デバイスドライバ２０２－１～２０２－ｎ」など、複数あり得る構成部分のいずれかを特定せずに示すときには、単に、「デバイスドライバ２０２」などとも記す。

【００２２】

ＯＳ２およびユーティリティプログラム３０は、例えば、記録媒体１１４（図３）を介してコンピュータ１に供給され、実行される。

ＯＳ２は、これらの構成部分により、プロセス２００－１～２００－ｍ（ｍ≧１）を実行し、ユーティリティプログラム３０から設定されるアクセス規則に従って、図３に示した表示・入力装置１０６などのデバイスに対するアクセスを制御する。

また、ユーティリティプログラム３０は、図２を参照して説明したように、同一のデバイスに対して複数の経路からアクセスがあるときに、この経路ごとに作成されたデバイスファイル（図２）それぞれに対するアクセス規則を統一し、ＯＳ２に設定する。

【００２３】

ＯＳ２において、デバイスドライバ２０２は、デバイスファイルを介してプロ

セス２００のアクセスを受け、表示・入力装置１０６などのデバイスを動作させる。

ファイルシステム２０４は、ディレクトリごとにファイル（デバイスファイルを含む）を記憶し、管理する。

デバイスＤＢ２０６は、デバイスと、そのデバイス番号とを対応付けて記憶し、管理する。

【００２４】

デバイスファイルＤＢ２０８は、デバイスファイルと、デバイス番号とを対応付けて記憶し、管理する。

ディレクトリ管理部２１０は、ファイルシステム２０４内のディレクトリを管理する。

【００２５】

規則ＤＢ２１４は、ファイルシステム２０４内のディレクトリそれぞれに設定されるデバイスファイルへのアクセス規則の設定を受け、設定されたアクセス規則を記憶し、管理する。

規則ＤＢ２１４に設定されるアクセス規則は、上述のように、デバイスファイルに対するアクセスが、読み出しのみについて許可されているか、書き込みのみについて許可されているか、これらの両方について許可されているか、あるいは、これらの両方について禁止されているかを、ファイルシステム２０４内のディレクトリあるいはデバイスファイルごとに規定する。

なお、規則ＤＢ２１４に対しては、コンピュータ１の表示・入力装置１０６（図３）に対するユーザの設定操作により、あるいは、ユーティリティプログラム３０からの通知により、アクセス規則が設定される。

【００２６】

アクセス制御部２１２は、規則ＤＢ２１４に記憶されているアクセス規則に従って、プロセス２００からデバイスファイルへのアクセス、および、プロセス２００とデバイスファイルとの間の経路にあり、デバイスファイルとリンクされたファイルからデバイスファイルへのアクセスを制御する。

プロセス実行部２１６は、プロセス２００を実行する。

【００２７】

ユーティリティプログラム３０において、検索部３０２は、デバイスファイルＤＢ２０８を検索し、デバイスファイルと、そのデバイスファイルに対応するデバイスのデバイス番号などを示す情報を得る。

デバイス番号生成部３００は、デバイスファイルＤＢ２０８に対する検索の結果として得られた情報を解析し、デバイスファイルに対応するデバイスのデバイス番号を生成する。

規則抽出部３０４は、規則ＤＢ２１４を検索し、デバイスファイルそれぞれに対するアクセスについて、ディレクトリあるいはデバイスファイルごとに設定されたアクセス規則を抽出する。

【００２８】

規則導出部３０６は、抽出されたアクセス規則の内、同じデバイスファイルに対する複数のディレクトリからのアクセスについて設定されたアクセス規則を、例えば、上述したように、最もデバイスファイルに対するアクセスの条件が厳しくなるように統一するように、アクセス規則を導出する。

また、あるいは、規則導出部３０６は、複数のアクセス規則のいずれかに、全てのアクセス規則を統一するように、アクセス規則を導出する。

あるいは、規則導出部３０６は、デバイスファイルにリンクされたファイルの性質に応じて統一するように、アクセス規則を導出する。

このように、規則導出部３０６は、同一のデバイスに対応する複数のデバイスファイルに対する各ディレクトリのアクセス規則が統一されるように、各デバイスごとにアクセス規則を導出し、ＯＳ２の規則ＤＢ２１４に記憶させる。

【００２９】

[第１のユーティリティプログラム３０の動作]

図５は、図４に示した第１のユーティリティプログラム３０の動作（Ｓ１０）を示すフローチャートである。

ＯＳ２側でデバイスファイルに対するアクセスが生じると、ＯＳ２のアクセス制御部２１２が、第１のユーティリティプログラム３０に対して、アクセスされたデバイスファイルを示す情報を含むアクセス規則導出依頼を発行する。

図５に示すように、ステップ１００（Ｓ１００）において、ユーティリティプログラム３０は、ＯＳ２からアクセス規則導出依頼が来たか否かを判断する。

ユーティリティプログラム３０は、アクセス規則導出依頼が来たときにはＳ１０２の処理に進み、これ以外のときにはＳ１００の処理に留まる。

【００３０】

ステップ１０２（Ｓ１０２）において、検索部３０２は、ＯＳ２のデバイスファイルＤＢ２０８を検索し、全てのデバイスファイルの情報を得る。

デバイス番号生成部３００は、検索の結果として得られたデバイスファイルの情報それぞれから、デバイスファイルに対応するデバイスのデバイス番号を取り出す。

【００３１】

ステップ１０４（Ｓ１０４）において、規則抽出部３０４は、取り出されたデバイス番号から、アクセスされたデバイスファイルに対応するデバイスのデバイス番号と同じデバイス番号を検索する。

ステップ１０６（Ｓ１０６）において、規則抽出部３０４は、検索の結果として、アクセスされたデバイスファイルに対応するデバイスのデバイス番号と同じデバイス番号が複数、見つかったか否かを判断する。

ユーティリティプログラム３０は、検索の結果として同じデバイス番号が複数あったときにはＳ１０８の処理に進み、これ以外のときにはＳ１１４の処理に進む。

【００３２】

ステップ１０８（Ｓ１０８）において、規則抽出部３０４は、ＯＳ２の規則ＤＢ２１４を検索し、Ｓ１０６の処理において複数、見つかったデバイス番号のデバイスにアクセスする全てのデバイスファイルに対して設定されたアクセス規則の情報を得る。

規則抽出部３０４は、検索の結果として見つかった情報からアクセス規則を抽出する。

【００３３】

ステップ１１０（Ｓ１１０）において、規則導出部３０６は、抽出されたアク

セス規則を統一するアクセス規則を導出する。

つまり、規則導出部３０６は、上記デバイス番号のデバイスに対応する複数のデバイスファイルにリンクされた複数のファイルを含む複数のディレクトリそれぞれに対して設定されるアクセス規則を統一する。

【００３４】

ステップ１１２（Ｓ１１２）において、規則導出部３０６は、導出されたアクセス規則をＯＳ２に通知する。

Ｓ１１２の処理による通知を受けたＯＳ２の規則ＤＢ２１４は、通知に従ってアクセス規則を変更し、アクセス制御部２１２は、変更されたアクセス規則に従って、デバイスファイルに対するアクセスを制御する。

ステップ１１４（Ｓ１１４）において、規則導出部３０６は、アクセス規則の変更がない旨をＯＳ２に通知する。

この場合は、ＯＳ２の規則ＤＢ２１４は、アクセス規則を変更しない。

【００３５】

［ＯＳ２の動作］

次に、ＯＳ２のアクセス制御に関する動作を説明する。

図６は、図４に示したＯＳ２のアクセス制御に関する動作（Ｓ１２）を示す図である。

図６に示すように、ステップ１２０（Ｓ１２０）において、ＯＳ２のアクセス制御部２１２は、プロセス２００あるいはデバイスファイルにリンクされたファイルが、デバイスファイルに対するアクセスのために、ファイルオープンを要求したか否かを判断する。

ＯＳ２は、ファイルオープンの要求があったときにはＳ１２２の処理に進み、これ以外のときにはＳ１２０の処理に留まる。

【００３６】

ステップ１２２（Ｓ１２２）において、アクセス制御部２１２は、ユーティリティプログラム３０に対してアクセス規則導出依頼を発行する。

このアクセス規則導出依頼を受けると、ユーティリティプログラム３０は、図５に示した処理を実行する。

ステップ１２４（Ｓ１２４）において、規則ＤＢ２１４は、ユーティリティプログラム３０から、アクセス規則の通知（Ｓ１１２，Ｓ１１４；図５）を受けたか否かを判断する。

ＯＳ２は、アクセス規則の通知を受けたときにはＳ１２６の処理に進み、これ以外のときにはＳ１２４の処理に留まる。

【００３７】

ステップ１２６（Ｓ１２６）において、規則ＤＢ２１４は、ユーティリティプログラム３０からの通知が、アクセス規則の変更があることを示しているか否かを判断する。

ＯＳ２は、ユーティリティプログラム３０からの通知がアクセス規則の変更があることを示しているときにはＳ１２８の処理に進み、これ以外のときにはＳ１３０の処理に進む。

ステップ１２８（Ｓ１２８）において、規則ＤＢ２１４は、ユーティリティプログラム３０からの通知に従って、アクセス規則を変更して記憶・管理する。

【００３８】

ステップ１３０（Ｓ１３０）において、アクセス制御部２１２は、デバイスファイルに対するアクセスが、規則ＤＢ２１４に記憶されているアクセス規則に適合するか否かを判断する。

ＯＳ２は、デバイスファイルへのアクセスがアクセス規則に適合している場合にはＳ１３２の処理に進み、これ以外の場合にはＳ１３４の処理に進む。

【００３９】

ステップ１３２（Ｓ１３２）において、アクセス制御部２１２は、デバイスファイルのファイルオープンのための処理を行う。

ステップ１３４（Ｓ１３４）において、アクセス制御部２１２は、デバイスファイルに対するアクセスを拒否する。

【００４０】

［全体動作］

以下、ＯＳ２およびーティリティプログラム３０の全体的な動作を説明する。

図７は、図４に示したＯＳ２および第１のユーティリティプログラム３０の全

体的な動作（Ｓ１４）を示すシーケンス図である。

図７に示すように、ステップ１４０（Ｓ１４０）において、プロセス２００は、直接、あるいは、ファイルを介して、ＯＳ２に対してデバイスファイルのファイルオープンを要求する。

【００４１】

ステップ１４２（Ｓ１４２）において、ＯＳ２は、ユーティリティプログラム３０に対して、規則導出を依頼する。

ステップ１４６（Ｓ１４６）において、ユーティリティプログラム３０は、ＯＳ２に対して、デバイスファイルの検索など、アクセス規則の導出に必要な処理を行う。

【００４２】

ステップ１４８（Ｓ１４８）において、ユーティリティプログラム３０は、アクセス規則を導出すると、導出した規則をＯＳ２に通知する。

ステップ１５０（Ｓ１５０）において、ＯＳ２は、ユーティリティプログラム３０から通知された規則に従って、デバイスファイルに対するアクセスを許可し、あるいは、不許可にする。

【００４３】

［第２実施形態］

以下、本発明の第２の実施形態を説明する。

第１の実施形態として、デバイスファイルへのアクセスが生じるたびに、ＯＳ２から第１のユーティリティプログラム３０に対して規則導出を依頼する方法を説明した。

しかしながら、この方法によると、デバイスファイルへのアクセスが発生するたびに、ユーティリティプログラム３０によるアクセス規則の導出が行われるので、デバイスファイルにアクセスするために時間がかかり、また、処理付加も大きい。

本発明の第２の実施形態は、このような点を解決するために、ＯＳ２の起動時に、全体的なアクセス規則の導出を行い、その後は、ＯＳ２のアクセス規則の変更が生じたときに、第２のユーティリティプログラム３２（図８を参照して後述

）によるアクセス規則の導出を行うように改良されている。

【００４４】

図８は、第２のユーティリティプログラム３２の構成を示す図である。

なお、図８に示した第２のユーティリティプログラム３２の構成部分の内、図４に示したユーティリティプログラム３０の構成部分と実質的に同じものには、同じ符号が付されている。

図８に示すように、第２のユーティリティプログラム３２は、第１のユーティリティプログラム３０（図４）に、差分規則導出部３２０を付加した構成を採る。

【００４５】

第２のユーティリティプログラム３２も、第１のユーティリティプログラム３０と同様に、記録媒体１１４などを介してコンピュータ１に供給され、実行される。

差分規則導出部３２０は、ＯＳ２からアクセス規則導出依頼を受けたときに、アクセス規則が変更されたアクセスファイル（差分）について、アクセス規則の導出を行う。

【００４６】

［ＯＳ２および第２のユーティリティプログラム３２の動作］

以下、第２の実施形態におけるＯＳ２および第２のユーティリティプログラム３２の動作を説明する。

図９は、第２のユーティリティプログラム３２起動時の動作（Ｓ１６）を示すフローチャートである。

なお、図９に示した各処理の内、図５に示した処理と実質的に同じものには同じ符号が付されている（以下の各図について同じ）。

ＯＳ２が起動されると、ＯＳ２は、ユーティリティプログラム３２を起動する。

【００４７】

図９に示すように、ステップ１６０（Ｓ１６０）において、ユーティリティプログラム３２の検索部３０２は、ＯＳ２の規則ＤＢ２１４に記憶されている全て

のアクセス規則、および、デバイスファイルＤＢ２０８に記憶されている全てのデバイスファイルを取得する。

ステップ１６２（Ｓ１６２）において、デバイス番号生成部３００は、Ｓ１６０の処理において得られたデバイスファイルの情報からデバイス番号を抽出する。

【００４８】

ステップ１６４（Ｓ１６４）において、規則抽出部３０４は、Ｓ１６２の処理により得られたデバイス番号に基づいて、デバイスそれぞれに対応するデバイスファイルを抽出する。

ステップ１６６（Ｓ１６６）において、規則抽出部３０４は、共通のデバイスに対応して複数のデバイスファイルが設けられているか、つまり、規則導出の対象となるデバイスがあるか否かを判断する。

【００４９】

ユーティリティプログラム３２は、規則導出の対象となるデバイスがある場合にはＳ１０８の処理に進み、これ以外の場合にはＳ１１４の処理に進む。

Ｓ１０８～Ｓ１１４（図５を参照）の処理において、ユーティリティプログラム３２は、アクセス規則の導出およびＯＳ２に対する規則の通知を行う。

【００５０】

図１０は、図９に示した第２のユーティリティプログラム３２の処理により規則の通知を受けたＯＳ２の動作（Ｓ１８）を示すフローチャートである。

ステップ１８０（Ｓ１８０）において、ＯＳ２の規則ＤＢ２１４は、ユーティリティプログラム３２からの規則を受信する。

ステップ１８２（Ｓ１３２）において、規則ＤＢ２１４は、ユーティリティプログラム３２の通知に従って、アクセス規則を変更して記憶・管理する。

これ以降、アクセス制御部２１２は、規則ＤＢ２１４に記憶・管理されたアクセス規則に従ってアクセス制御を行う。

【００５１】

図１１は、アクセス規則の変更に関するＯＳ２の動作（Ｓ２０）を示すフローチャートである。

図１２は、ＯＳ２によるアクセス制御の動作（Ｓ２２）を示すフローチャートである。

図１１に示すように、規則ＤＢ２１４は、アクセス規則を変更する設定がなされたか否かを判断する。

ＯＳ２は、アクセス規則を変更する設定がなされたときにはＳ２０２の処理に進み、これ以外の場合にはＳ２００の処理に留まる。

なお、アクセス規則が変更される場合には、上述のように、規則ＤＢ２１４に対する設定変更の他に、アクセス制御部２１２によるディレクトリ構成の変更、あるいは、デバイスＤＢ２０６に対するデバイス設定の変更なども含まれる。

【００５２】

ステップ２０２（Ｓ２０２）において、アクセス制御部２１２は、ユーティリティプログラム３２に対して、アクセス規則が変更されたデバイスファイルについての情報（差分情報；アクセス規則が変更されたデバイスファイルおよびそれらに対応するデバイスのデバイス番号など）を含むアクセス規則変更依頼を発行する。

このアクセス規則変更依頼を受けると、ユーティリティプログラム３２は、差分についてのアクセス規則の導出（図１３を参照して後述）を行い、ＯＳ２に対して導出結果を通知する。

Ｓ１２４～Ｓ１２８の処理（図６）において、規則ＤＢ２１４は、ユーティリティプログラム３２からのアクセス規則の通知に従って、アクセス規則を変更し、あるいは、変更しないままとする。

アクセス制御部２１２は、図１２に示すＳ１２０，Ｓ１３０，Ｓ１３２（図６）の処理において、以上のように変更され、あるいは変更されないままとされたアクセス規則に従って、アクセス制御を行う。

【００５３】

図１３は、図１１に示したＯＳ２の処理（Ｓ２０）により、アクセス規則の導出依頼を受けた第２のユーティリティプログラム３２の処理（Ｓ２４）を示すフローチャートである。

図１３に示すように、ステップ２４０（Ｓ２４０）において、ユーティリティ

プログラム３２は、ＯＳ２からのアクセス規則導出依頼を受けたか否かを判断する。

ユーティリティプログラム３２は、アクセス導出依頼を受けた場合にはＳ２４２の処理に進み、これ以外の場合にはＳ２４０の処理に留まる。

【００５４】

ステップ２４２（Ｓ２４２）において、デバイス番号生成部３００は、ＯＳ２から受けた差分情報からデバイス番号を取り出す。

ステップ２４４（Ｓ２４４）において、Ｓ２４２の処理により取り出されたデバイス番号に、同一のデバイス番号が複数あるいか否かを判断する。

ユーティリティプログラム３２は、同一のデバイス番号が複数あるときにはＳ２４６の処理に進み、これ以外のときにはＳ２５０の処理に進む。

【００５５】

ステップ２４６（Ｓ２４６）において、差分検出部３２０は、アクセス規則が変更されたデバイスファイル（差分）に対応するデバイスについて、統一のアクセス規則を導出する。

ステップ２４８（Ｓ２４８）において、差分規則導出部３２０は、差分について導出したアクセス規則をＯＳ２に対して通知する。

ステップ２５０（Ｓ２５０）において、差分規則導出部３２０は、差分についてアクセス規則が変更されない旨をＯＳ２に通知する。

【００５６】

［ＯＳ２および第２のユーティリティプログラム３２の全体動作］

以下、ＯＳ２および第２のユーティリティプログラム３２の全体的な動作を説明する。

図１４は、ＯＳ２およびユーティリティプログラム３２（図８）の起動時の全体的な動作（Ｓ２６）を示すフローチャートである。

ＯＳ２が起動されると、図１４に示すように、ステップ２６０（Ｓ２６０）において、ＯＳ２は、ユーティリティプログラム３２を起動する。

【００５７】

ステップ２６２（Ｓ２６２）において、ユーティリティプログラム３２は、規

則ＤＢ２１４およびデバイスファイルＤＢ２０８を検索し、アクセス規則導出に必要な情報を取得する。

ステップ２６４（Ｓ２６４）において、ユーティリティプログラム３２は、ＯＳ２に対して、導出したアクセス規則を通知する。

【００５８】

図１５は、アクセス規則に変更が生じたときのＯＳ２およびユーティリティプログラム３２（図８）の全体的な動作（Ｓ２８）を示すフローチャートである。

アクセス規則の変更が生じると、図１５に示すように、ステップ２８０（Ｓ２８０）において、ＯＳ２は、ユーティリティプログラム３２に対して、差分情報を含むアクセス規則導出依頼を発行する。

ユーティリティプログラム３２は、このアクセス規則導出依頼を受けて、図１３に示したように、差分についてアクセス規則を導出する。

ステップ２８２（Ｓ２８２）において、ユーティリティプログラム３２は、差分について導出されたアクセス規則をＯＳ２に通知する。

【００５９】

【発明の効果】

以上説明したように、本発明に係るアクセス制御システムおよびその方法によれば、コンピュータのＯＳの脆弱性を手当てして、その安全性を向上させることができる。

【図面の簡単な説明】

【図１】

本発明の背景を、具体例を挙げて説明する図である。

【図２】

本発明の概要を、具体例を挙げて説明する図である。

【図３】

本発明に係るアクセス制御方法が適応されるコンピュータのハードウェア構成を例示する図である。

【図４】

図３に示したコンピュータ上で動作するＯＳの構成と、本発明に係るアクセス

制御方法を実現する第１のユーティリティプログラムの構成を示す図である。

【図５】

図４に示した第１のユーティリティプログラムの動作（Ｓ１０）を示すフローチャートである。

【図６】

図４に示したＯＳのアクセス制御に関する動作（Ｓ１２）を示す図である。

【図７】

図４に示したＯＳおよび第１のユーティリティプログラムの全体的な動作（Ｓ１４）を示すシーケンス図である。

【図８】

第２のユーティリティプログラムの構成を示す図である。

【図９】

第２のユーティリティプログラムの起動時の動作（Ｓ１６）を示すフローチャートである。

【図１０】

図９に示した第２のユーティリティプログラムの処理により規則の通知を受けたＯＳの動作（Ｓ１８）を示すフローチャートである。

【図１１】

アクセス規則の変更に関するＯＳの動作（Ｓ２０）を示すフローチャートである。

【図１２】

ＯＳによるアクセス制御の動作（Ｓ２２）を示すフローチャートである。

【図１３】

図１１に示したＯＳの処理（Ｓ２０）により、アクセス規則の導出依頼を受けた第２のユーティリティプログラムの処理（Ｓ２４）を示すフローチャートである。

【図１４】

ＯＳおよびユーティリティプログラム（図８）の起動時の全体的な動作（Ｓ２６）を示すフローチャートである。

【図１５】

アクセス規則に変更が生じたときのＯＳおよびユーティリティプログラム（図８）の全体的な動作（Ｓ２８）を示すフローチャートである。

【符号の説明】

１・・・コンピュータ、

１００・・・本体、

１０２・・・ＣＰＵ、

１０４・・・メモリ、

１０６・・・表示・入力装置、

１１０・・・通信装置、

１１２・・・記録装置、

１１４・・・記録媒体、

２・・・ＯＳ、

２００・・・プロセス、

２０２・・・デバイスドライバ、

２０４・・・ファイルシステム、

２０６・・・デバイスＤＢ、

２０８・・・デバイスファイルＤＢ、

２１０・・・ディレクトリ管理部、

２１２・・・アクセス制御部、

２１４・・・規則ＤＢ、

２１６・・・プロセス実行部、

３０，３２・・・ユーティリティプログラム、

３００・・・デバイス番号生成部、

３０２・・・検索部、

３０４・・・規則抽出部、

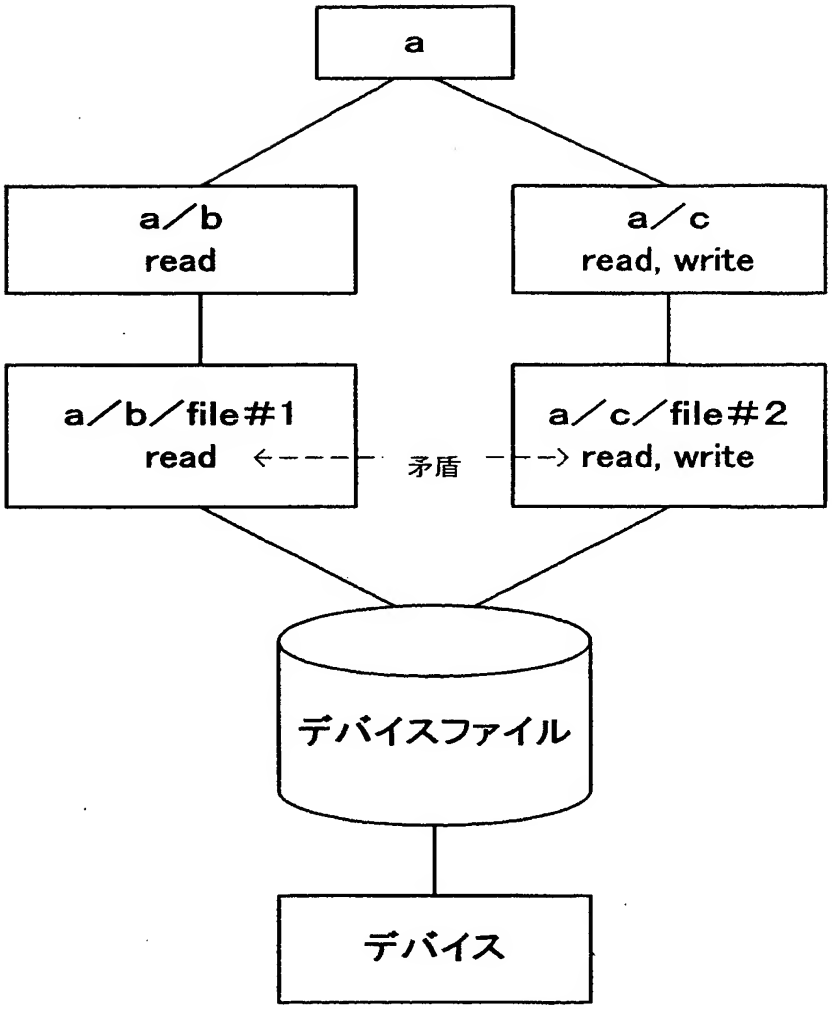
３０６・・・規則導出部、

３０８・・・規則ＤＢ、

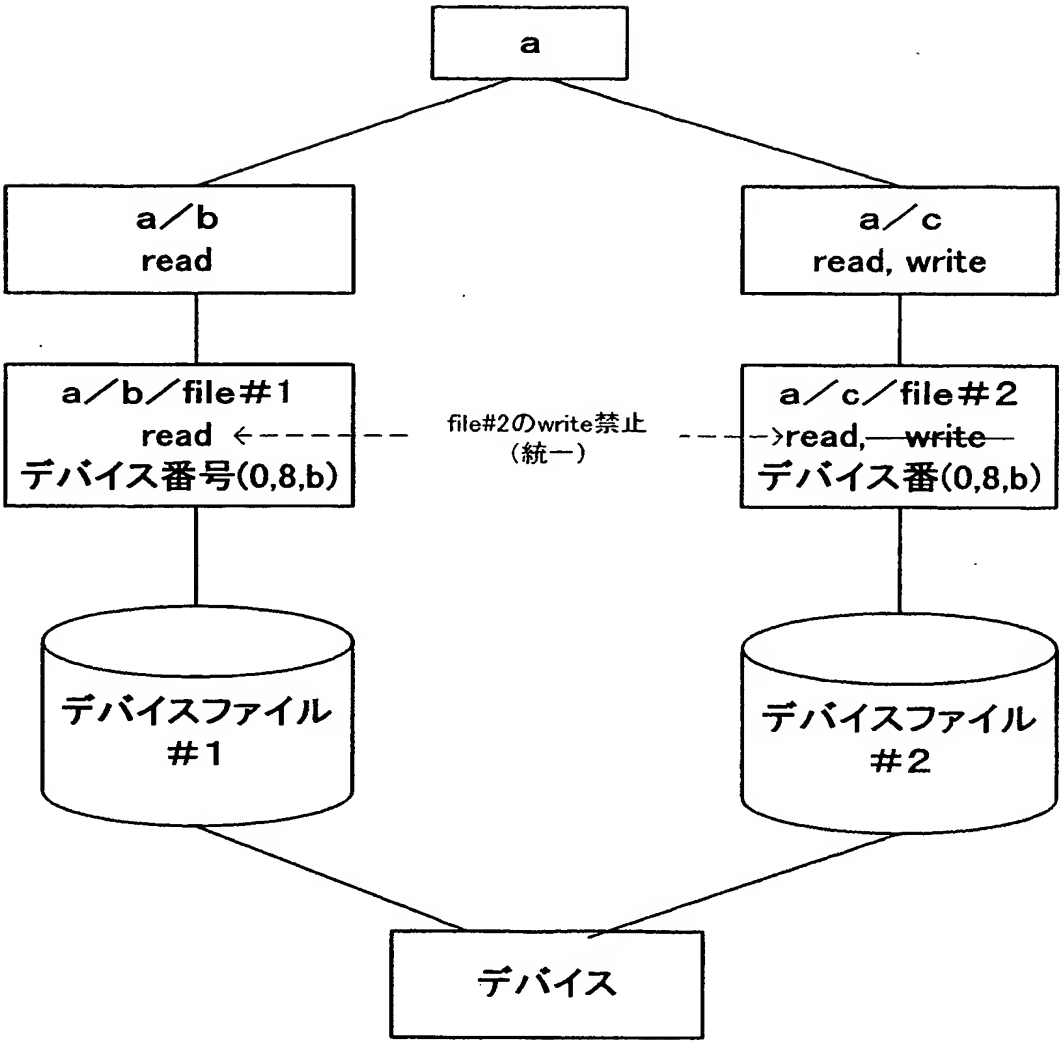
３２０・・・差分規則導出部、

【書類名】　図面

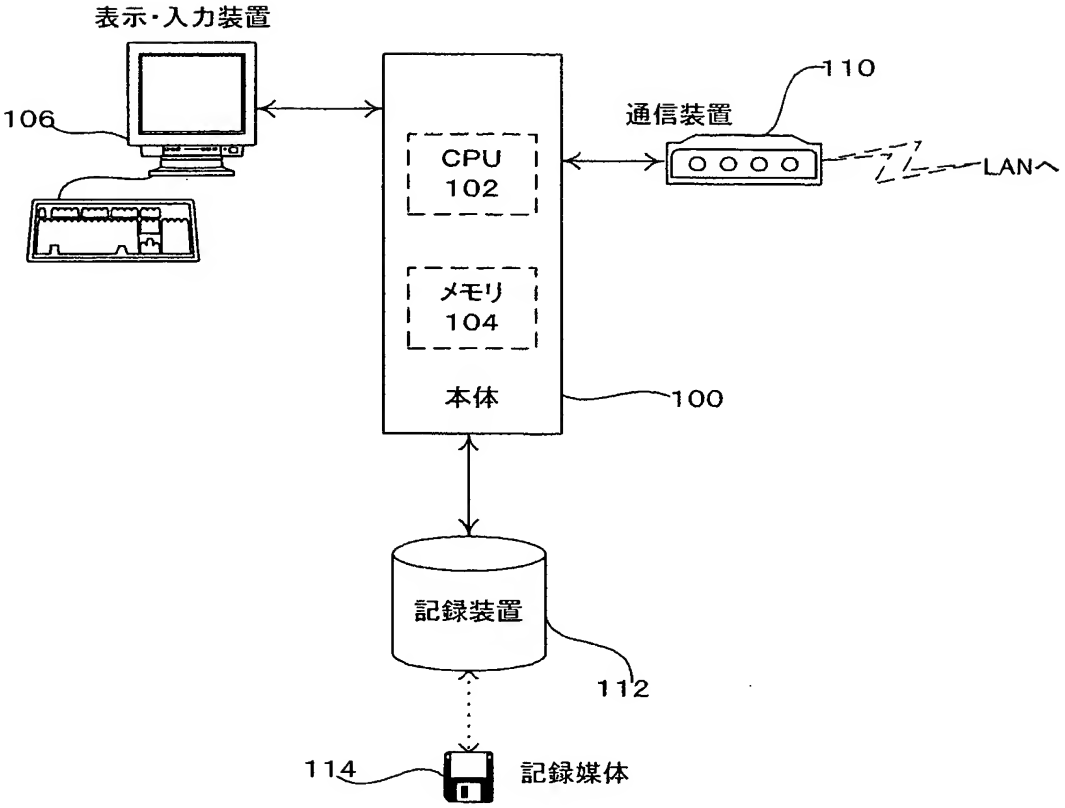
【図１】


a
a／b
read
a／c
read, write
a／b／file#1
read
矛盾
a／c／file#2
read, write
デバイスファイル
デバイス

【図２】

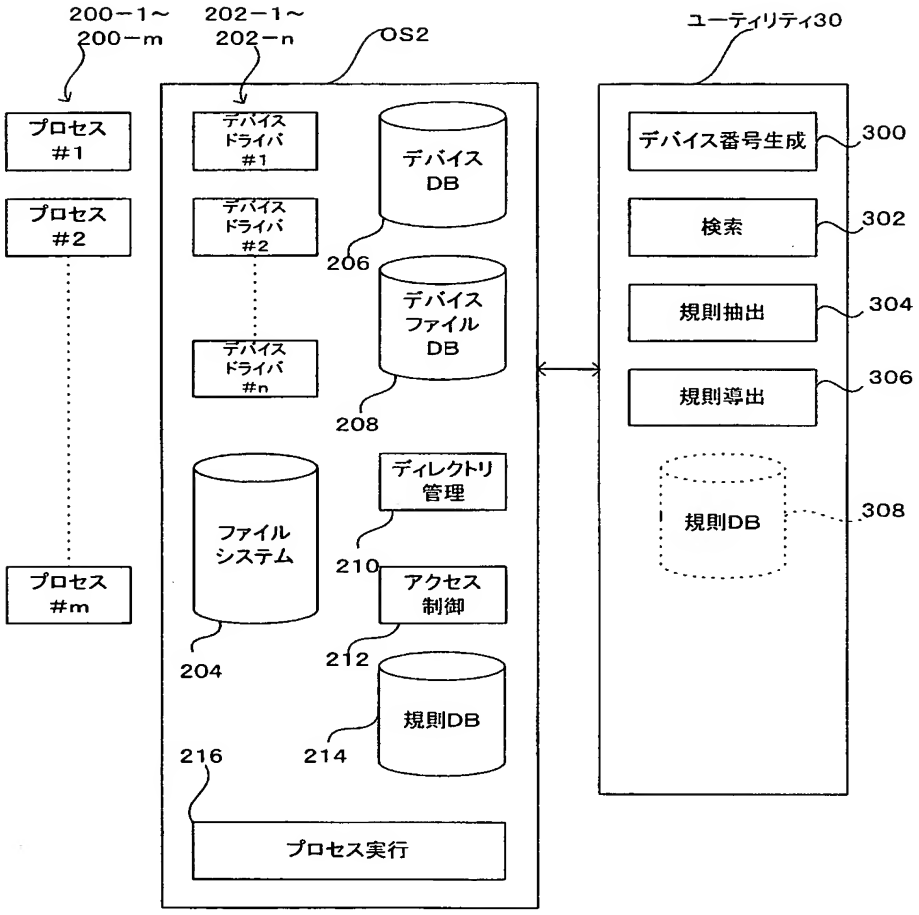

a
a／b
read
a／c
read, write
a／b／file#1
read
デバイス番号(0,8,b)
file#2のwrite禁止
(統一)
a／c／file#2
read, write
デバイス番(0,8,b)
デバイスファイル
#1
デバイスファイル
#2
デバイス

【図３】

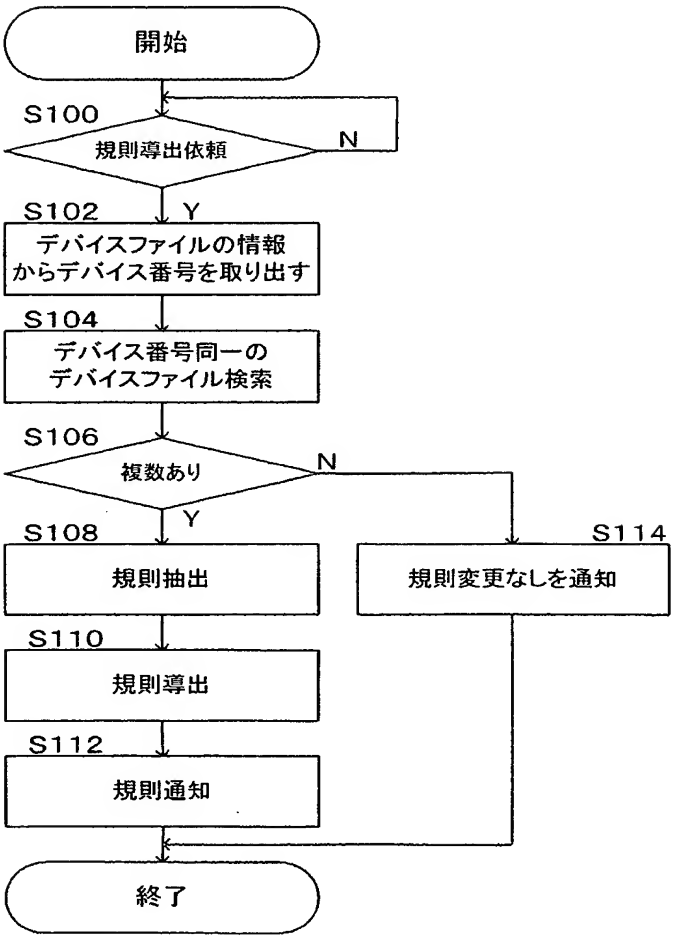

表示・入力装置
106
CPU
102
メモリ
104
本体
100
通信装置
110
LANへ
記録装置
112
114
記録媒体

コンピュータ1

【図４】

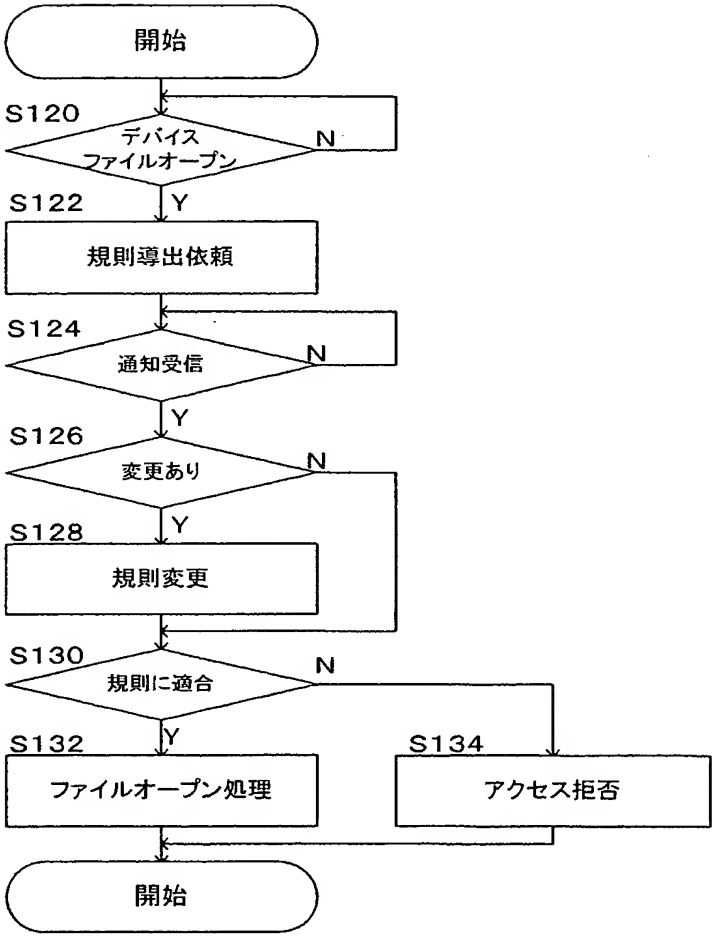

200−1〜
200−m
202−1〜
202−n
OS2
ユーティリティ30
プロセス
#1
プロセス
#2
プロセス
#m
デバイス
ドライバ
#1
デバイス
ドライバ
#2
デバイス
ドライバ
#n
デバイス
DB
206
デバイス
ファイル
DB
208
ファイル
システム
204
ディレクトリ
管理
210
アクセス
制御
212
規則DB
214
216
プロセス実行
デバイス番号生成
300
検索
302
規則抽出
304
規則導出
306
規則DB
308

【図５】


開始
S100
規則導出依頼
N
Y
S102
デバイスファイルの情報
からデバイス番号を取り出す
S104
デバイス番号同一の
デバイスファイル検索
S106
複数あり
N
Y
S108
規則抽出
S114
規則変更なしを通知
S110
規則導出
S112
規則通知
終了

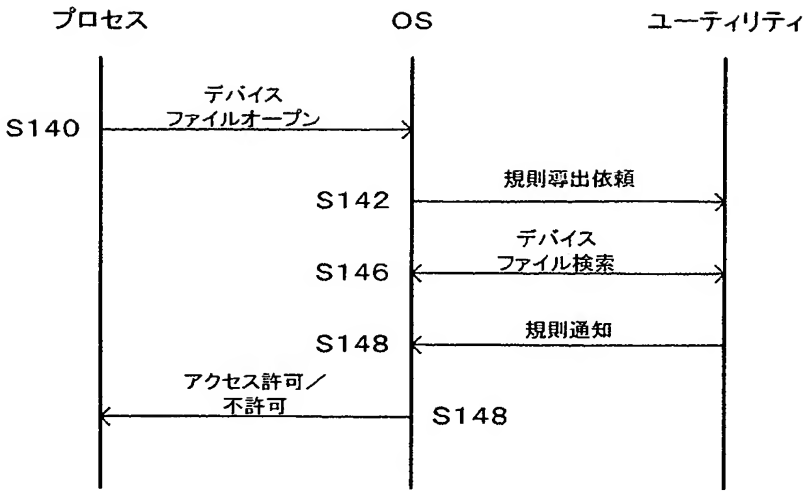
S10

【図６】


開始
S120
デバイス
ファイルオープン
N
Y
S122
規則導出依頼
S124
通知受信
N
Y
S126
変更あり
N
Y
S128
規則変更
S130
規則に適合
N
Y
S132
ファイルオープン処理
S134
アクセス拒否
開始

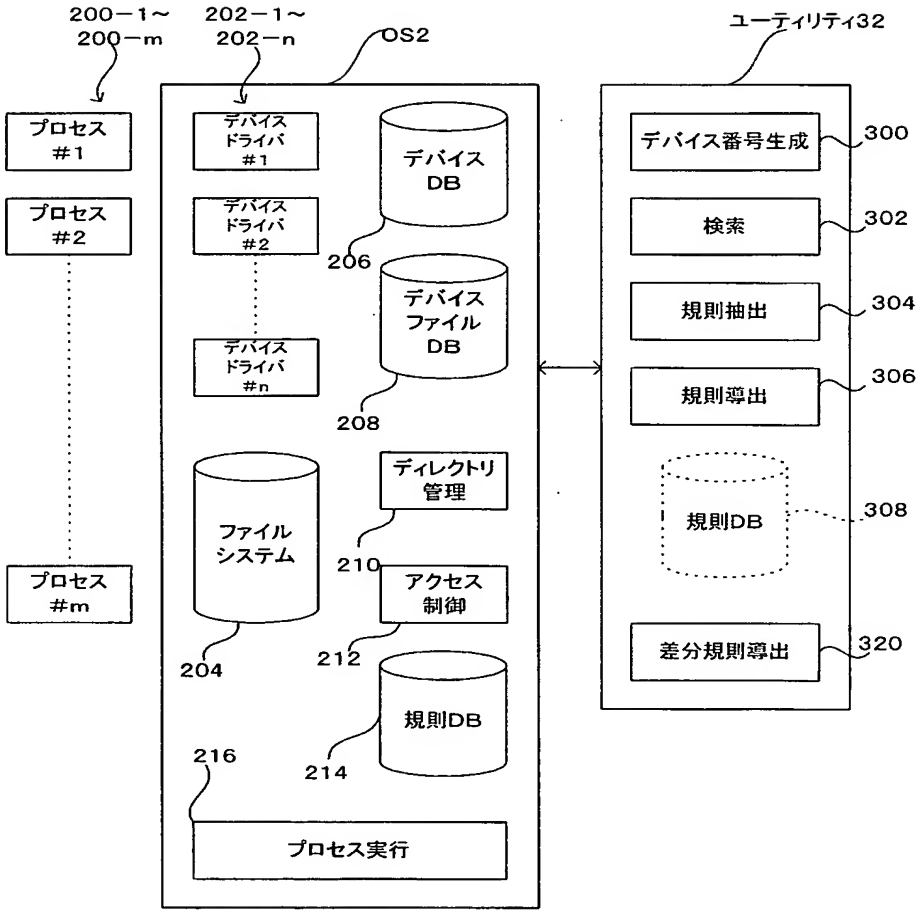
S12

【図７】

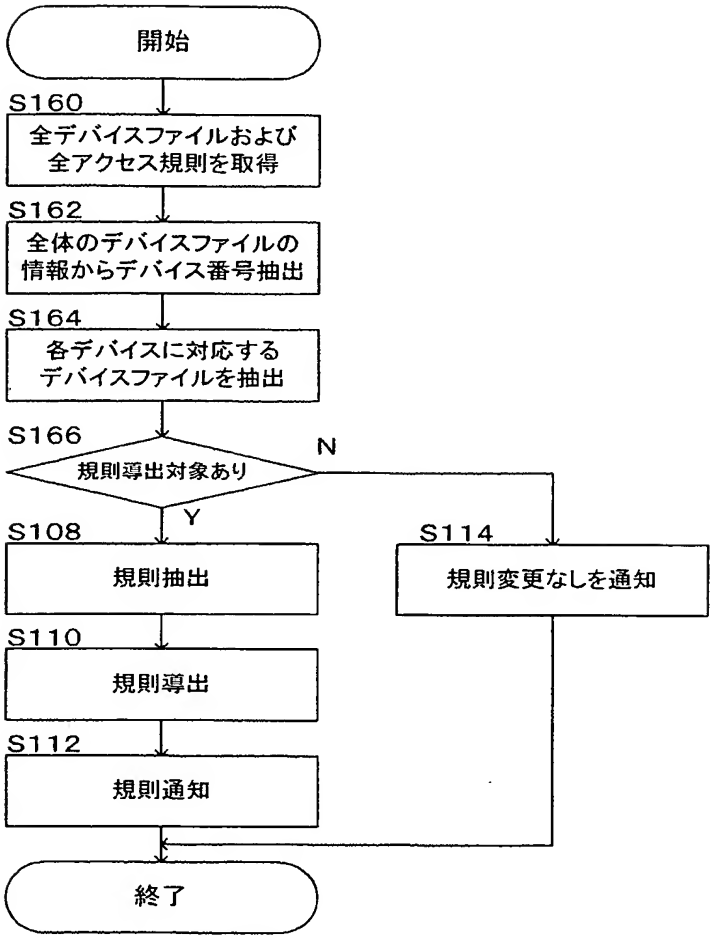

プロセス
OS
ユーティリティ
S140
デバイス
ファイルオープン
S142
規則導出依頼
S146
デバイス
ファイル検索
S148
規則通知
アクセス許可／
不許可
S148

S14

【図８】

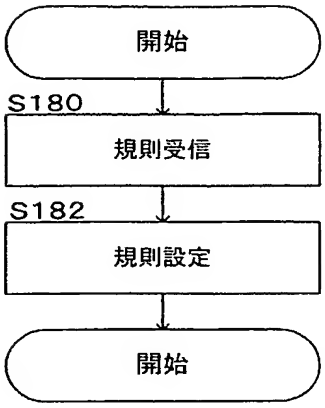

200－1～
200－m
202－1～
202－n
OS2
ユーティリティ32
プロセス
#1
プロセス
#2
プロセス
#m
デバイス
ドライバ
#1
デバイス
ドライバ
#2
デバイス
ドライバ
#n
デバイス
DB
206
デバイス
ファイル
DB
208
ファイル
システム
204
ディレクトリ
管理
210
アクセス
制御
212
規則DB
214
216
プロセス実行
デバイス番号生成
300
検索
302
規則抽出
304
規則導出
306
規則DB
308
差分規則導出
320

【図９】


開始
S160
全デバイスファイルおよび
全アクセス規則を取得
S162
全体のデバイスファイルの
情報からデバイス番号抽出
S164
各デバイスに対応する
デバイスファイルを抽出
S166
規則導出対象あり
N
Y
S108
規則抽出
S110
規則導出
S112
規則通知
S114
規則変更なしを通知
終了

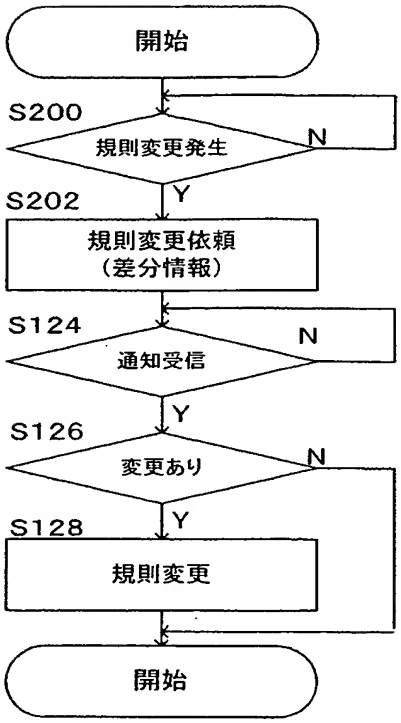
S16

【図１０】



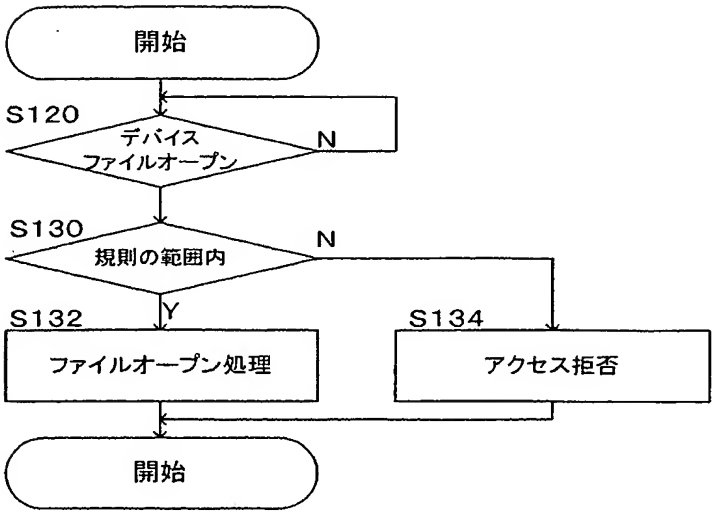
S18

【図１１】


開始
S200
規則変更発生
N
Y
S202
規則変更依頼
（差分情報）
S124
通知受信
N
Y
S126
変更あり
N
Y
S128
規則変更
開始

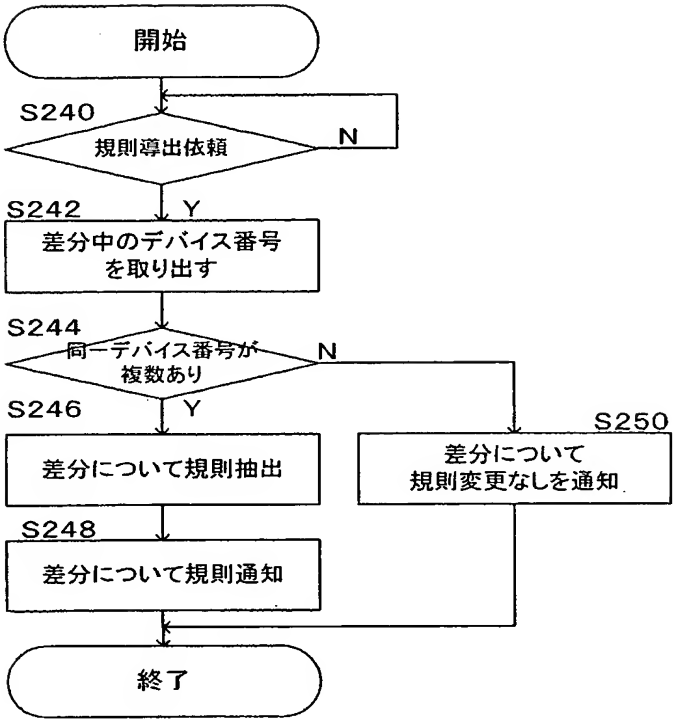
S20

【図１２】


開始
S120
デバイス
ファイルオープン
N
S130
規則の範囲内
N
Y
S132
ファイルオープン処理
S134
アクセス拒否
開始

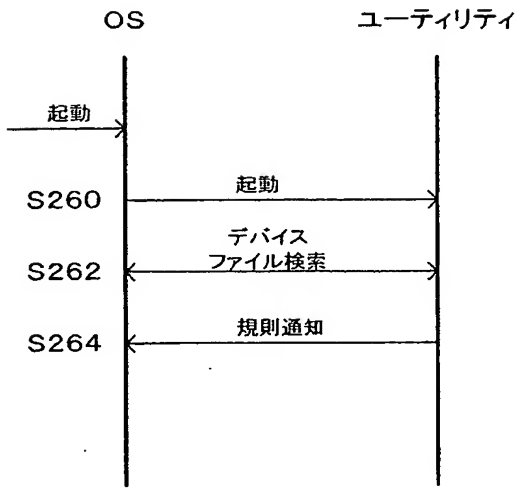
S22

【図１３】


開始
S240
規則導出依頼
N
Y
S242
差分中のデバイス番号
を取り出す
S244
同一デバイス番号が
複数あり
N
Y
S246
差分について規則抽出
S248
差分について規則通知
S250
差分について
規則変更なしを通知
終了

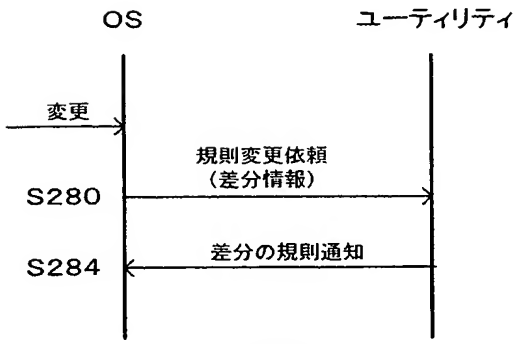
S24

【図１４】



S26

【図１５】



S28

【書類名】　　要約書

【要約】

【課題】コンピュータのＯＳの脆弱性を手当てして、その安全性を向上させる。

【解決手段】プロセスが、同じデバイスにアクセスするときの経路それぞれにデバイスファイルを置き、これら複数のデバイスファイルに対するアクセス規則を統一する。例えば、あるプロセスからデバイスにアクセスするための経路が２つあるときには、これらの経路それぞれにデバイスファイル＃１，＃２を置く。これらのデバイスファイルにアクセスする全てのディレクトリ（ａ／ｂ，ａ／ｃ）に対して設定されるアクセス規則を読み出し（ｒｅａｄ）のみに統一し、２つの経路のいずれからも、同じ規則に従って、デバイスファイルがアクセスされるようにする。

【選択図】　　図２

特願２００３－１０４７５６

出　願　人　履　歴　情　報

識別番号　［３９９１１７１１０］

１．変更年月日　１９９９年１０月１３日
［変更理由］　新規登録
住　所　東京都杉並区高井戸東３丁目２９番２１号
氏　名　日本ヒューレット・パッカード株式会社